



July 26, 2019

Robert Cordle
Chair, North Carolina State Board of Elections
430 N. Salisbury St.
Raleigh, NC 27603
bob.cordle.board@ncsbe.gov

Re: NCSBE's Consideration of Certification of Voting Systems on July 28, 2019

Chair Cordle:

I write on behalf of Protect Democracy, a non-partisan non-profit organization that works to defend democratic norms and institutions. We write to respectfully request that the North Carolina State Board of Elections ("NCSBE" or "the Board") refrain from certifying any new ballot-marking device voting systems at its public meeting this Sunday, July 28, 2019.

Earlier this week, the Board announced that its July 28 meeting will include consideration of whether to certify three voting systems for use in North Carolina elections. There are complex questions relating to the security, accuracy, and usability of those systems. Before reaching a certification decision on any of those systems, the Board should ensure that there is adequate opportunity for public consideration and commentary, as well as time for the Board to consult with experts and continue gathering information.

As the Board knows, implementing secure and reliable voting systems—the very infrastructure of our democracy—is more important than ever. Just yesterday, the U.S. Senate Select Committee on Intelligence issued a report outlining the sweeping and continuing threat of sophisticated foreign attacks on our country's election systems. Among other things, it concluded that "Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure." We know the Board shares that sense of urgency. Accordingly, it should ensure that it—and the public—have ample opportunity to consider the potential benefits and pitfalls of any new election system, particularly any system that does not rely on hand-marked paper ballots.

Background

On July 22, 2019, NCSBE notified the public that it will hold a meeting on July 28, 2019, to address several agenda items, including whether to certify new voting systems pursuant to

N.C.G.S. § 163A-1115(a) (eff. December 2019 statewide).¹ Three companies are currently seeking certification for ballot-marking device (BMD) voting systems:

1. Clear Ballot, headquartered in Massachusetts, for its ClearVote 1.4 system;
2. ES&S, based in Nebraska, for its EVS 5.2.2.0 system; and
3. Hart InterCivic, based in Texas, for its Verity Voting 2.2 system.²

Security and Operational Risks of BMDs

Compared to the hand-marked paper ballots used by a majority of North Carolina voters, BMD systems introduce unnecessary security and operational risks into the voting process. BMD systems typically consist of a computerized device used to mark a paper ballot (the BMD itself) and a computerized device used to tabulate the paper ballots.³ A voter uses a BMD to fill out their ballot, the BMD prints a paper ballot reflecting the voter's choices, and the completed ballot is fed into a tabulator to count votes.

Experts have identified several security risks associated with BMDs. *First*, BMDs operate on computer systems, thus increasing the attack surface available to potential hackers (especially when compared to hand-marked paper ballots).⁴ *Second*, some BMD systems, including ES&S's ExpressVote system, print barcodes on ballots which are then read by the tabulator. Some researchers have argued that barcodes can be manipulated to instruct a scanner to flip or otherwise alter votes.⁵ Because people cannot read barcodes, a voter has no way of knowing whether their ballot has been altered.⁶ *Third*, even when a BMD system does not use a bar code, one study has shown that half of all voters do not review their printed ballot after voting on a BMD, and those who do spend an average of 4 seconds doing so.⁷ For these and

¹ Notice of Meeting, N.C. St. Bd. of Elections, (July 22, 2019), https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2019-07-28/Meeting_Notice_2019-07-28.pdf.

² N.C. St. Bd. of Elections, *Voting Options: Elections & Voting Systems*, <https://www.ncsbe.gov/Voting-Options/Elections-Voting-Systems>, (last visited July 25, 2019).

³ See generally Nat'l Conf. of St. Legislatures, *Voting Equipment* (Aug. 20, 2018), <http://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx>.

⁴ Andrew Appel, Richard A. Demillo & Philip B. Stark, *Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters* (Apr. 21, 2019), available at <https://ssrn.com/abstract=3375755>.

⁵ Jennifer Cohn, *Will Georgia Double Down On Non-Transparent, Vulnerable Election Machines?*, Who.What.Why. (Jan. 2, 2019), <https://whowhatwhy.org/2019/01/02/will-georgia-double-down-on-non-transparent-vulnerable-election-machines/>.

⁶ Jennifer Cohn, *What Is the Latest Threat to Democracy? Bar-Codes and Ballot Marking Devices A.K.A. "Electronic Pencils,"* Medium (Mar. 6, 2018), <https://medium.com/@jennycohn1/what-is-the-latest-threat-to-democracy-ballot-marking-devices-a-k-a-electronic-pencils-16bb44917edd>.

⁷ Appel *et al.*, *supra* note 4, at 9–10.

other reasons, the United States Department of Homeland Security is currently assessing the potential risks of BMDs.⁸

Setting aside the security risks of BMDs, their computerized features give rise to unnecessary operational risks. Glitches in the software or hardware of BMDs and power failures can either prevent voters from using the machines—thereby increasing wait times at polling places—or lead to inaccurate ballots. Additionally, BMD devices typically impose far greater costs on counties than systems that rely on hand-marked paper ballots, both at the initial procurement stage and over time.

We note that in many instances it may be helpful to maintain a BMD system in counties that use hand-marked paper ballots in order to assist voters with disabilities—and indeed, all counties in North Carolina provide a BMD-based system for that purpose. We do not raise any concerns with the practices in those counties and expect that if more counties moved to a system based on hand-marked paper ballots they would accommodate all voters using currently-certified systems.

Additional Known Security Risks of ES&S's ExpressVote System

There are additional known security risks associated with ES&S's ExpressVote system that should counsel caution before certifying it for use in North Carolina. Indeed, three organizations recently petitioned Pennsylvania's Department of State to re-examine its recent certification of ES&S's ExpressVote XL voting system on ten separate grounds.⁹ Among other things, that petition states that security researchers have now discovered that the ExpressVote XL could either malfunction or be manipulated to add, modify, or invalidate votes after a voter has viewed, confirmed, and cast their ballot.¹⁰

In addition, the ExpressVote runs an outdated version of Windows, which will soon be vulnerable to attack. The overview of ES&S's North Carolina system available on NCSBE's website reports that several features of ES&S's system run on the Windows 7 operating system.¹¹ Less than two weeks ago, the Associated Press reported that ES&S still uses Windows 7 for its voting systems because it still has not received federal accreditation for upgrading its

⁸ Mark Niese, *DHS to Assess Risks Posed to Ballot-Marking Devices*, Atlanta Journal-Constitution (May 2, 2019), available at <https://www.govtech.com/security/DHS-to-Assess-Risks-Posed-to-Ballot-Marking-Devices.html>.

⁹ Letter from Ronald A. Fein, Legal Director of Free Speech for the People, *et al.* to Kathy Boockvar, Acting Secretary of the Commonwealth (July 16, 2019), https://freespeechforpeople.org/wp-content/uploads/2019/07/petition_for_reexamination_of_expressvote_xl.pdf.

¹⁰ See *id.* at PDF page 3 (Petition page 1) n.1 (collecting sources).

¹¹ ES&S, *ES&S Voting System 5.2.2.0: System Overview* at 12, 33, https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2019-06-13/Voting%20System%20Certification/ESS/ES%26S%20Overview_Redacted.pdf (last visited July 25, 2019).

systems to Windows 10.¹² Windows 7 was released in 2009 and reaches its end of life on January 14, 2020, meaning that Microsoft will generally stop providing technical support and fix software vulnerabilities.¹³

Potential Failure to Comply with State and Federal Requirements

In addition to raising serious security and operational concerns, at least some of the systems currently under consideration likely fail to satisfy the minimum requirements set forth by state and federal law and the NCSBE:

- NCSBE may only certify voting systems “if they generate either a paper ballot or a paper record *by which voters may verify their votes before casting them* and which provides a backup means of counting the vote that the voter casts.” N.C.S.G. § 163A-1115(a) (emphasis added). Similarly, § 3.4.2.6 of NCSBE’s *Election Systems Certification Program* manual (hereinafter, “NCSBE’s *Certification Manual*”)¹⁴ specifies that each voting system “must permit the voter to verify, in a private and independent manner, the vote selected by the voter on the ballot before the ballot is cast and counted.” NCSBE also receives funds under the Help America Vote Act (HAVA), and § 3.4.1.1 of NCSBE’s *Certification Manual* specifies that NCSBE may only certify voting systems that comply with HAVA Section 301. HAVA § 301(a)(1)(A)(i), codified at 42 U.S.C. § 21081(a)(1)(A)(i), requires that voting systems “permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted.” BMDs that use barcodes may not meet these requirements, as they fail to provide voters with any means of actually verifying their votes before casting them.
- Section 3.4.2.10 of NCSBE’s *Certification Manual* specifies that each “voting system must maintain the integrity of the vote by, at minimum, establishing processes and mechanisms necessary to protect the security of electronic tabulation processes, the paper ballot, and to prevent unauthorized access to any critical component of the voting system. It is the expectation of the State Board that voting systems include and maintain robust security mechanisms to preserve the integrity of the election process.” BMDs that are susceptible to hackers’ attempts to add, modify, or invalidate votes after a voter has cast their ballot may not meet this requirement.

¹² Tami Abdollah, *AP Exclusive: New Election Systems Use Vulnerable Software*, Associated Press (July 13, 2019), <https://www.apnews.com/e5e070c31f3c497fa9e6875f426ccde1>.

¹³ *Id.* While extended support may be available at additional cost to counties, it is not as comprehensive and provides only a temporary solution.

¹⁴ Available at https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2019-06-13/Voting%20System%20Certification/NCSBEVotingSystemsCertificationProgram_06132019.pdf.

Conclusion

For all of these reasons, we respectfully urge the Board not to make any decisions to certify any new voting system during this Sunday's public meeting. Before reaching those decisions, the Board should ensure ample opportunity for the public to receive information and submit comments to inform the Board's decision. We emphasize in particular that the Board should not vote on Sunday to certify the ExpressVote, which has been the subject of extensive (and recent) concern by researchers and voters across the country. We would be happy to provide any further information that might be helpful.

Sincerely,

A handwritten signature in dark ink, appearing to read "Larry Schwartz", is positioned above the typed name.

Larry Schwartz
Counsel, Protect Democracy

CC: Stella Anderson, Secretary
Kenneth Raymond, Member
Jeff Carmon III, Member
David C. Black, Member